

Cisco – Creating Core Dumps

Table of Contents

<u>Creating Core Dumps</u>	1
<u>Introduction</u>	1
<u>Before You Begin</u>	1
<u>Conventions</u>	1
<u>Prerequisites</u>	1
<u>Components Used</u>	1
<u>Creating Core Dumps</u>	2
<u>Basic Setup</u>	2
<u>Using File Transfer Protocol</u>	3
<u>Using Remote Copy Protocol</u>	4
<u>Using a Flash Disk</u>	4
<u>Using Trivial File Transfer Protocol</u>	4
<u>Advanced Setup</u>	5
<u>Exception Memory</u>	5
<u>Debug Sanity</u>	6
<u>Testing the Core Dump Setup</u>	6
<u>Related Information</u>	6

Creating Core Dumps

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

Creating Core Dumps

Basic Setup

Using File Transfer Protocol

Using Remote Copy Protocol

Using a Flash Disk

Using Trivial File Transfer Protocol

Advanced Setup

Exception Memory

Debug Sanity

Testing the Core Dump Setup

Related Information

Introduction

This document explains the various options you can use to enable core dumps in Cisco IOS® software.

Note: Core dumps can be difficult to obtain and should only be interpreted by Cisco technical personnel who have access to source code and detailed memory maps. On many platforms, core dumps may not be necessary if the crashinfo feature is used. See Retrieving Information from the Crashinfo File for more information.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

Readers of this document should be knowledgeable about:

- [Troubleshooting Router Crashes](#)

Components Used

The information in this document is based on the software version below:

- Cisco IOS Software Version 12.0 and later

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live

network, ensure that you understand the potential impact of any command before using it.

Creating Core Dumps

When a router crashes, it can be useful to obtain a copy of the router's entire memory contents (called a core dump) for your technical support representative to use to identify the cause of the crash. Not all crashes produce a core dump. For more details, see [Types of Crashes](#).

Always capture the console logs when the router is attempting to dump a core. The console logs provide information about the crash. In addition, the ROM Monitor (ROMMON) normally prints information to the console (and only to the console) at the time of the crash.



Caution: Core dumps are not needed to solve most crash cases. Creating a core dump while the router is functioning in a network can disrupt network operation. Use the commands discussed in this document only under the direction of a technical support representative.

Basic Setup

There are four basic ways to set up the router to generate a core dump:

- Using File Transfer Protocol (FTP)
- Using Remote Copy Protocol (RCP)
- Using a Flash Disk
- Using Trivial File Transfer Protocol (TFTP)

Each of these methods uses the following configuration commands:

```
exception region-size size  
  
exception core-file filename [compress]
```

Use the **exception region-size** command to define a small amount of memory to serve as a fallback pool when the processor memory pool is marked corrupt. This helps to prevent memory failures during the core dump process. The *size* parameter is expressed in bytes and can be configured from 1024 to 65536 bytes, with a default value of 16384 bytes. Configure the **exception region-size** as 65536 bytes to increase the chance of a successful core dump.

By default, the processor memory core dump is written to a file named "*hostname*-core", where *hostname* is the name of the router defined by the **hostname** configuration command. If the router has Input/Output (I/O) memory (for example, the Cisco 7200), an I/O memory core dump may also be created, written to the file "*hostname*-coreiomem".

Use the **exception core-file** command to override the default core dump filename. If the file server has a DOS FAT file system, do not specify a file name longer than six characters. For example, if you configure a

router with "**exception core-file** *foobar*", the processor memory core dump is named "foobar" and the I/O memory dump is named "foobario" (enough to give you a hint that you have an I/O memory dump).

Make sure there is enough disk space on the file server to hold multiple complete core dumps. Core dump files can be compressed with the **compress** option.

Note: Compress is used automatically when writing core dump files to Flash disk; the **compress** option is not supported when writing core dump files using RCP.

Using File Transfer Protocol

Note: File Transfer Protocol (FTP) is the recommended method for configuring a core dump.

To configure the router for a core dump using FTP, use the following commands:

- **ip ftp username** *username*
- **ip ftp password** *password*
- **exception protocol ftp**
- **exception region-size** *65536*
- **exception dump** *ip-address*

Note: To avoid congesting your network, it is highly recommended that the router be directly connected to the FTP server, with no intermediate hops. If you must go through one or more intermediate hops, you may need to use the **ip ftp source-interface** command to specify which interface will be used to access the FTP server. See Configuring a Router to Use FTP Connections for more information.

If the username and password above are not configured, the router attempts anonymous FTP.

When requested by a Cisco technical support representative, you can send core dump files to Cisco via anonymous ftp. The ftp server is ftp-sj.cisco.com and the directory is /incoming (**Note:** this directory is invisible). Make sure to set the transfer mode to binary. If the files are not already compressed, consider compressing them with a common compression utility like gzip or zip.

Also make sure to include the crashinfo file if it was created along with the core dump (it should be if the hardware/software supports it). See Retrieving Information from the Crashinfo File for instructions on how to do this.

It's a good idea to make sure that FTP works first using the example below:

```
c7500#copy running-config ftp:
Address or name of remote host []? 172.18.125.3
Destination filename [c7500-config]?
Writing c7500-config !
2781 bytes copied in 0.944 secs
```

Using Remote Copy Protocol

To configure the router for a core dump using RCP, use the following commands:

- **ip rcmd remote-username** *username*
- **exception protocol rcp**
- **exception region-size** *65536*
- **exception dump ip-address**

If the username above is not configured, the router uses its hostname as the username for RCP.

Note: To avoid congesting your network, it is highly recommended that the router be directly connected to the RCP server, with no intermediate hops. If you must go through one or more intermediate hops, you may need to use the **ip rcmd source-interface** command to specify which interface will be used to access the RCP server. See *Configuring a Router to Use rsh and rcp* for more information.

It's a good idea to make sure that RCP works first by using the following example:

```
c7500#copy running-config rcp:
Address or name of remote host []? 172.18.125.3
Destination username [c7500]?
Destination filename [c7500-config]?
Writing c7500-config !
2781 bytes copied in 0.944 secs
```

Using a Flash Disk

Some router platforms support the Flash disk as an alternative to the linear Flash memory or PCMCIA Flash card. The large storage capacity of these Flash disks makes them a good medium for capturing a core dump. For information on the router platforms and Cisco IOS software versions that support the Flash disk, refer to the *Cisco IOS Release Notes*.

To configure a router for a core dump using a Flash disk, use the following command:

```
exception flash <procmem/iomem/all> <device_name[:partition_number]>
```

The **show flash all EXEC** command gives you a list of devices you can use for the **exception flash** command.

Using Trivial File Transfer Protocol

Due to a limitation of most TFTP applications, the router only dumps the first 16 MB of the core file. Therefore, if your router's main memory is larger than 16 MB, do not use TFTP. See *Cisco IOS TFTP Client Cannot Transfer Files Larger than 16MB in Size* for more information.

To configure a router for a core dump using TFTP, use the following:

-

exception protocol tftp

- **exception region-size** *65536*
- **exception dump** *ip-address*

TFTP is the default protocol for **exception protocol**.

Note: To avoid congesting your network, it is highly recommended that the router be directly connected to the TFTP server, with no intermediate hops. If you must go through one or more intermediate hops, you may need to use the **ip tftp source-interface** command to specify which interface will be used to access the TFTP server.

Depending on the TFTP server used, it may be necessary to create empty target file(s) with the appropriate permissions before the router can write to them.

It's a good idea to make sure that TFTP works first by using the following example:

```
c7500#copy running-config tftp:
Address or name of remote host []? 172.18.125.3
Destination filename [c7500-config]?
!
2781 bytes copied in 0.944 secs
```

Advanced Setup

The configuration commands in this section may be used in addition to those described in the Basic Setup section.

Exception Memory

To debug some memory problems, you can cause the router to create a core dump and reboot when certain memory size parameters are violated. The following **exception memory** commands are used to trigger a core dump:

- **exception memory minimum** *size* – forces a crash if the amount of free processor memory shrinks below the configured threshold.
- **exception memory fragment** *size* – forces a crash if the Cisco IOS software cannot allocate a contiguous processor memory block larger than the configured threshold.

The *size* parameter is expressed in bytes and is checked by default every 60 seconds.

These commands only cause the router to reboot when the configured conditions are met. With **exception dump** or **exception flash** also configured, the router creates a core dump first. These commands may be useful to diagnose memory leaks.

Debug Sanity

In some cases, the technical support representative will request that **debug sanity** be enabled when configuring the core dump. This is a hidden command in most Cisco IOS software releases and is sometimes necessary to debug memory corruption, especially I/O memory corruption. With **debug sanity** enabled, every buffer that is used in the system is sanity-checked when it is allocated, and again when it is freed.

The **debug sanity** command has to be issued in privileged EXEC mode (**enable** mode) and although it uses some CPU capacity, it does not significantly affect the router's functionality. Like other **debug** commands, **debug sanity** is not saved in the configuration and thus will not survive a reboot of the system.

Not all types of crashes require **debug sanity** to be enabled. Use this command only when your technical support representative requests it.

To disable sanity checking, use the privileged EXEC command **undebug sanity**.

Testing the Core Dump Setup

Once the router is configured for core dump, it may be useful to test the setup.

Cisco IOS software provides the special **write core** command in privileged EXEC mode (**enable** mode) to cause the router to generate a core dump without reloading.

If successful, the core dump file(s) will be the size of the the respective memory regions. It is important to remember that the entire memory region is dumped, not just the memory which is in use.

The **write core** command also may be useful if the router is malfunctioning, but has not crashed.

Related Information

- [Configuring a Core Dump on a GSR Line Card](#)
- [Troubleshooting Router Crashes](#)
- [Troubleshooting Router Hangs](#)
- [Troubleshooting Memory Problems](#)
- [Technical Support – Hardware Support](#)
- [Technical Support – Cisco Systems](#)

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jan 13, 2003

Document ID: 12687
